Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 02 June 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports the Energy Department has ordered a full review of security at Lawrence Livermore National Laboratory after discovering "unacceptable" security lapses. (See item 1)
- The Associated Press reports U.S. Customs authorities are investigating a sighting of three scuba divers near a Somerset, MA power plant early Saturday morning. (See item 2)
- The U.S. Department of Homeland Security in consultation with the Homeland Security Council, has lowered the national threat level from Code Orange or high risk of terrorist attack to Code Yellow or an elevated risk of terrorist attack. (See item 14)
- IDG News Service reports that Microsoft has issued updates to Security Bulletins MS03−007, which was originally released in March, and MS03−013, which was first released in April. (See item 25)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 01, New York Times* — **Security lapses found at nuclear laboratory.** The Energy Department has ordered a full review of security at Lawrence Livermore National Laboratory after discovering "unacceptable" security lapses. **Federal officials ordered the review of the laboratory in Northern California on Friday after learning that the loss of an electronic access badge had gone unreported to senior managers for six weeks. The badge could help**

gain access to 3,000 offices at the facility, some containing classified nuclear information. The electronic badge was lost by a security officer on a routine shift in mid−April, and several days later, security officers discovered that a set of keys to the gates of the weapons laboratory was also missing. Laboratory officials changed the locks, and they said they had no indication that anybody had used the keys or the electronic badge to gain entry. Linton Brooks, the national nuclear security administrator at the Energy Department, said the failure to report potentially serious security breaches "is unacceptable." **Brooks ordered a team from Washington to visit the laboratory beginning Monday and review security problems.** The team will also consider whether the Energy Department should assume direct management of security at Livermore, which is operated by the University of California.
Source: http://www.nytimes.com/2003/06/01/national/01SECU.html

2. *May 31, Associated Press* — **Authorities investigating suspicious divers seen near power plant. Authorities are investigating a sighting of three scuba divers near a Somerset, MA power plant early Saturday morning.** An employee of NRG Electric Generating Plant told police he spotted three scuba divers on a beach next to the northeast side of the plant shortly after midnight. When he called to them, they replied in a language that he didn't understand, said state police spokesman Tom Ryan. The three then fled leaving behind their scuba gear, he said. **Bomb disposal units from state police and the Federal Bureau of Investigation responded, but no explosives were found, Somerset police said. Ryan said there were no indications of terrorist activity. He said authorities suspected the divers were involved in illegal drug activity that may be related to a coal ship docked at the plant.** U.S. Customs is handling the investigation. Officials found additional diving equipment near the coal ship, U.S. Customs spokeswoman Janet Rapaport said.
Source: http://www.boston.com/dailynews/151/region/Authorities_inves tigating_susp:.shtml

3. *May 29, Reuters* — **Iowa to harness wind at compressed air power plant.** A novel project to wed wind energy with underground compressed air to produce electricity is planned for Iowa, a state aiming −− with a boost from billionaire investor Warren Buffett −− to become a big player in wind generation **A group of Iowa municipal electric and gas utilities plans to build a $200 million generating station based on a technology called compressed air energy storage, or CAES, near Fort Dodge, Iowa.** The Iowa Stored Energy Plant would store compressed air in an underground aquifer to be released and blended with natural gas to fire combustion turbines to make electricity for transmission over the state's power grid. Compressed air would replace about two−thirds of the gas normally burned in a turbine. **Backers said the stored energy could generate up to 200 megawatts of electricity, or power for about 200,000 homes.** Energy from a new 100 megawatt wind power farm would be tapped to run compressor motors to force air into the aquifer at a pressure of 500 pounds per square inch. **Wind turbines also could generate electricity for direct transmission over the grid, with 1 megawatt powering about 300 homes.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_natio nal.htm?SMDOCID=reuters_pma_2003_05_29_eng−reuters_pma_IOWA− TO−HARNESS−WIND−AT−COMPRESSED−AIR−POWER−PLANTa>

4. *May 29, Reuters* — **Canada approves New Brunswick−Maine power line. Canada's energy regulator said on Thursday it approved an application from NB Power for a C$75 million ($54 million) transmission line to Maine from the Point Lepreau nuclear plant in New**

Brunswick. But the National Energy Board said NB Power, New Brunswick's utility, must still get approvals for the U.S. portion of the line from federal and state regulators in the United States before it can start construction. At a hearing in March, NB Power said the 96 km (60 mile) power line would help provide system reliability in New Brunswick and improve New England's access to generating capacity. **The utility has more than enough capacity in southern New Brunswick to allow for exports, including the 1,000 Megawatt Coleson Cove plant, 265 MW of gas−fired plants, the 600 MW Point Lepreau station and 600 MW of hydro power, it has said.** Construction of the Canadian part of the project is expected to start near the end of 2005, the NEB said.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.htm?SMDOCID=reuters_pma_2003_05_29_eng−reuters_pma_CANADA−APPROVES−NEW−BRUNSWICK−MAINE−POWER−LINEa>

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

Nothing to report.
[Return to top]

Transportation Sector

5. *May 31, Federal Computer Week* — **Group proposes CAPPS II alternative. The creation of a two−tiered passenger screening and registered traveler program could serve as an alternative to the controversial computer system that combs databases to assess the risk posed by individual airline passengers,** according to a report issued last week. The Reason Public Policy Institute, a Los Angeles−based think tank, proposed a risk−based alternative to the Transportation Security Administration's Computer Assisted Passenger Prescreening System (CAPPS) II. **The group's system would check each traveler's information against terrorist watch lists and airline databases and separate travelers into two groups based on risk. Under the proposal, frequent travelers could become registered travelers and breeze through checkpoints by opting for extensive background checks, including employment and credit history. High−risk travelers would have their boarding passes electronically flagged and receive extra scrutiny, although they would wait in the same lines as ordinary travelers.** TSA officials have discussed the registered traveler option as a future extension of the CAPPS II program. Frequent travelers would be given identification cards with biometric

data, such as iris scans or face geometry, which would be confirmed before boarding. Medium−risk travelers — which would include most passengers — and high−risk travelers would be screened in the same lines.
Source: http://www.govexec.com/dailyfed/0503/053003t1.htm

6. *May 30, Associated Press* — **US Airways has possible home in Pennsylvania. U.S. Senator Arlen Specter says he plans to discuss the possibility of US Airways shifting its offices to Pennsylvania in exchange for improvements at Pittsburgh and Philadelphia airports.** The senator's willingness to court the Arlington based carrier follows comments made by U.S. Airways president David Siegel about leaving Virginia, if it doesn't start receiving better treatment from Reagan Washington National Airport. But US Airways officials backed off Siegel's statements yesterday. Spokesman David Castleveter says Siegel was merely noting the airline's growing popularity after emerging from bankruptcy. **Pennsylvania officials are scheduled to meet with US Airways executives June 11th to go over the airline's demands for improvements at Pittsburgh and Philadelphia airports.**
Source: http://www.wusatv9.com/news/news_article.asp?storyid=18839

[Return to top]

Postal and Shipping Sector

7. *May 30, Associated Press* — **Postal Service postpones anthrax tests. A 14−city test of a new anthrax detection system planned for Monday, June 2 is being postponed, the Postal Service said.** The system, which uses rapid DNA testing to detect the germs, was developed in the wake of the anthrax−by−mail attacks in the fall of 2001 that killed five people and sickened many more. The 30−day test had been scheduled after the system was tried out in Baltimore for several months. However, postal vice president Azeezaly Jaffer said Friday that more time was needed to work with the Centers for Disease Control and Prevention and local authorities in the test cities to develop coordinated guidelines for responding to the test results. The detection systems have been installed in the 14 cities and are ready for use, he said. **No new date to begin the tests was announced.**
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−anthrax−test,0,439710.story?coll=sns−ap−nation−headlines

8. *May 26, Chemical &Engineering News* — **Postal Service readies defense: team will install PCR−based systems to detect biohazards in mail facilities. The U.S. Postal Service has awarded an initial $175 million contract to make and install biohazard detection systems in mail−sorting facilities nationwide.** At the heart of the system is a polymerase chain reaction (PCR)−based detector. The process will eliminate the need for sample handling. The PCR process−−sample preparation, DNA amplification, and detection−−is also automated. The detector has been designed for use by a minimally skilled operator in a nonlaboratory setting. **Successful testing of the system concluded early this year. The goal was to identify biothreats, such as anthrax, accurately in 30 minutes or less with no false positives and an insignificant level of inconclusive readings,** a spokesperson for the contractor said.
Source: http://pubs.acs.org/cen/topstory/8121/8121notw5.html

[Return to top]

Agriculture Sector

9. *May 30, dc.internet.com* — **NASA, USDA team for high tech agriculture tools. The U.S. Department of Agriculture (USDA) and NASA are teaming to bring technologies such as remote sensing to the American farmer.** The five−year agreement permits the USDA to draw on NASA's expertise in monitoring, mapping, modeling and systems engineering. According the USDA, the primary purpose of the project is to help increase the production efficiency of farmers while reducing the cost of production by **bringing more practical benefits of science and technology into agricultural applications.** USDA Secretary Ann M. Veneman said the technological advances available to farmers from precision agriculture techniques include monitors and maps that can detect and record changes in yields, soil attributes or crop conditions, including pest infestations and water nutrient stress. "NASA's unique ability to view the Earth from space will enhance our ability to predict climate, weather and natural hazards, as well as **to mitigate and assess the effects of natural and human−induced disasters**," said NASA Administrator Sean O'Keefe.
   Source: http://dc.internet.com/news/article.php/2214901

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

10. *May 30, Associated Press* — **City lifts 'boil water' notification.** Declaring tap water in Corpus Christi, TX safe to drink, city officials lifted the boil water notification that had been imposed for several days. Texas Commission of Environmental Quality regulations require utilities whose water pressure drops below 20 pounds per square inch to issue a boil water notice. **A leaking water main wrought havoc across the city for days.** The lack of water pressure forced schools and restaurants to close and companies to rent portable toilets. City officials said they had plugged the hole that was discovered Monday. **The 3−foot round cast iron pipe dates to 1954 and may have ruptured because of its old age, city spokesman Ted Nelson said.** He said that the city had already been laying a 5−foot wide replacement pipe as part of a multiyear, multimillion dollar improvement to its water system.
    Source: http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/193117 5

11. *May 30, Rocky Mountain News* — **Feds launch water talks with eye on distant future. The federal agency that built dams across the West will start a series of conferences in Denver, CO on June 6 to discuss water supplies**, but no new federally funded dams are on the agenda. "There is no money for building new dams," Bennett Raley, assistant interior secretary for water, said Wednesday. **"The areas where there are pressures for more water are going to be the ones that pay for the infrastructure when it is required to meet water needs,"** he said. Norton recently announced "Water 2025: Preventing Crises and Conflict in the West," a

program to address the emerging need for more water as a consequence of explosive population growth. John Keys, the current commissioner of the Bureau of Reclamation, said the mission is to find ways to conserve water and work with state and local officials to stretch supplies.
Source: http://rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_1998835,00.html

[Return to top]

Public Health Sector

12. *May 30, Associated Press* — **China denies SARS cover up in Beijing. A top Chinese health official denied claims that Beijing tried to hide the seriousness of the SARS virus, saying Friday, May 30 that the Chinese government warned about SARS as early as February and early efforts to fight it were slowed by poor information.** Gao Qiang, the executive deputy health minister in China, presented a copy of the Communist Party newspaper People's Daily, which reported about an atypical pneumonia Feb. 12 that had killed five people in Guangdong province and infected 305. The symptoms were similar to what now is known as severe acute respiratory syndrome, including fever, dry cough and chills, Gao said. The World Health Organization believes that SARS originated in Guangdong. "Infectious diseases are impossible to cover up," Gao said. "You may be able to cover up figures, but you can never cover up viruses." **Gao's comments were the highest−level response yet to accusations that communist officials tried to cover up the extent of the illness.** Critics have complained that China's early reluctance to release information might have worsened the impact of the disease. **Gao repeated official explanations that an inadequate Chinese public health network was to blame for earlier underreporting of the true scale of China's outbreak.** "The Chinese government did not conceal the truth," Gao said.
Source: http://abcnews.go.com/wire/Living/ap20030530_594.html

13. *May 30, 9news.com (Denver)* — **State health department reports second case of hantavirus. A 26−year−old farm worker from Alamosa County, CO has contacted hantavirus, a sometimes deadly infection spread by infected deer mice.** The man was transferred to a hospital in New Mexico where he is in stable condition. **This is the second confirmed case of hantavirus in Colorado this year,** according to the Colorado state health department. The first case was fatal. A 22−year−old man who contacted the virus died in January. Hantavirus is contacted by breathing in virus−contaminated dust from the feces, urine or saliva of infected deer mice. It can be contacted at any time of year, but is more common during the spring and summer months when people are opening up summer cabins or working in barns, sheds or grain silos where deer mice are present.
Source: http://www.9news.com/storyfull−newsroom.asp?id=14928

[Return to top]

Government Sector

14. *May 30, U.S. Department of Homeland Security* — **Statement by Secretary of Homeland Security Tom Ridge on lowering the threat level.** The Department of Homeland Security, in

consultation with the Homeland Security Council, has lowered the national threat level from Code Orange or high risk of terrorist attack to Code Yellow or an elevated risk of terrorist attack. **This decision is based upon a number of factors including a review of the intelligence and assessment of threats. The U.S. intelligence community has also concluded that the number of indicators and warnings that led to raising the level have decreased and the heightened vulnerability associated with the Memorial Day holiday has passed.**
Source: http://www.dhs.gov/dhspublic/display?content=857

15. *May 30, Government Executive* — **Terrorism course proves popular with federal managers.** Federal executives are lining up to take an Army course that teaches strategies for coping with the management issues posed by terrorism. **The one−day course, developed by the Army's Edgewood Chemical Biological Center at Aberdeen Proving Ground, MD, provides a basic overview of chemical and biological weapons and strategies for continuity of operations planning. It also includes tabletop exercises that allow managers to practice responding to terrorist incidents.** Federal managers in Minnesota took the course in January, and since then Edgewood has offered the course to executives in Washington,DC, Albuquerque, NM, and Philadelphia, PA. Edgewood officials are coordinating with federal executive boards across the country to plan future courses.
Source: http://www.govexec.com/dailyfed/0503/053003p1.htm

16. *May 30, Federal Computer Week* — **Sharing information. Four initiatives are under way to open up government agencies' internal networks so data can move more freely from employee to employee.** The CIA is responsible for Intelink, the FBI for Law Enforcement Online (LEO), the State Department for OpenNet and the Justice Department for the Regional Information Sharing Systems (RISS) network. While these networks now enable hundreds of thousands of government users to access classified and unclassified information, a great deal of work remains to be done before all of the data needed during an investigation is available via a few keystrokes. **The remaining tasks have less to do with daunting technical challenges and more to do with getting greater interagency coordination, amendments to current laws, new agency procedures and changes in employees' outlooks.**
Source: http://www.fcw.com/supplements/homeland/2003/sup2/hom−challenge−06−02−03.asp

17. *May 29, Bureau of Citizenship and Immigration Services* — **BCIS begins offering online filing for two popular immigration forms.** The Bureau of Citizenship and Immigration Services (BCIS) started accepting electronic filing (e−filing) of two of the most commonly submitted immigration forms − the application used to renew or replace a "green card"" (Form I−90) and the Application for Employment Authorization (Form I−765). Together, both forms represent approximately 30 percent of the 7 million applications filed with the Bureau every year. For those who file electronically, BCIS confirms the identity of the customer early in the application process. **BCIS also electronically collects a photograph, signature, and fingerprint for the individual. These biometric data are stored and can be used later for verification of the person's identity.** Customers whose applications are approved receive high quality immigration documents with special security features produced from BCIS' centralized card production facility.
Source: http://www.immigration.gov/graphics/publicaffairs/newsrels/e filing−052903.htm

18. *May 29, Reuters* — **U.S. plans search for student visa violators.** The U.S. Department of Homeland Security will be ready by Aug. 1 to begin searching for thousands of foreign nationals who may have violated the terms of their student visas, an official said. **But Chris Bentley, spokesman for Homeland Security's Bureau of Immigration and Customs Enforcement, said authorities would concentrate on suspected risks to national security rather than try to go after everyone suspected of a visa violation.** Bentley said as many as 10,000 people may have violated the terms of their student visas, double the 5,000−strong force of federal agents available to enforce immigration rules. Violations often occur when visa holders leave school for work without notifying immigration authorities. Violators face detainment and deportation.
Source: http://www.nytimes.com/reuters/news/news−attack−students.htm l

19. *May 29, U.S. Department of Justice* — **Justice Department releases 2001−2002 operations report for the National Instant Criminal Background Check System.** Attorney General John Ashcroft directed the FBI in 2001 and 2002 to take steps to ensure that NICS background checks are able to determine more thoroughly and efficiently whether a prospective gun buyer is entitled to obtain firearms. **Responding to a February 2002 directive of the Attorney General, the FBI implemented both temporary and permanent NICS procedures to include a check of records on the immigration status of non−immigrant aliens seeking to buy guns.**
Source: http://www.justice.gov/opa/pr/2003/May/03_ag_314.htm

[Return to top]

Emergency Services Sector

20. *May 29, Federal Emergency Management Agency* — **President Bush appoints former White House official as FEMA Chief Of Staff.** Patrick Rhode, a Hot Springs, AR, native who previously served in the Bush White House, has been appointed by President Bush to be chief of staff for the Federal Emergency Management Agency (FEMA), Under Secretary Michael D. Brown announced on Thursday. **As chief of staff, he is responsible for the day−to−day operations of the agency and for directing the implementation of Brown's priorities and policies. FEMA coordinates federal disaster relief activities, including the response and recovery operations of 26 federal agencies and departments and the American Red Cross.**
Source: http://www.fema.gov/nwz03/nwz03_rhode.shtm

[Return to top]

Information and Telecommunications Sector

21. *May 30, internetnews.com* — **Security disclosure debate reignites.** Online security consultancy **Spi Dynamics has sparked a new debate over the responsible handling of vulnerability warnings with the release of an alert for multiple security holes in the Sun ONE Application Server 7.0 without the availability of a patch or workaround from Sun Microsystems**. A spokesperson for Sun said one of the bugs has already been fixed in Update 1

of Application Server 7.0. **"The other three bugs will be fixed in Update 2, expected to be available in August**," the spokesperson told internetnews.com. **However, a JSP source code disclosure vulnerability which carries a "High" severity rating is still unpatched**. According to Spi Dynamics CEO Brian Cohen, since March 18 Sun's security unit responded once to say the holes were being patched but they needed time because the developer was on vacation. Since then, he said numerous attempts to get an update from Sun were unsuccessful. The Sun spokesperson denied Cohen's claim. "Spi was notified in previous communications of Sun's plan to fix these bugs," she said. The alert may be viewed at the Spi Dynamics Website: http://www.spidynamics.com/sunone_alert.html
Source: http://www.internetnews.com/dev−news/article.php/2214731

22. *May 30, Government Computer News* — **Study finds technical errors in government sites. A survey of 41 federal Web sites found that 68 percent will present some sort of bug within the first 15 minutes of a visit**, according to the Business Internet Group of San Francisco. Most glitches were application server and Web server errors such as blank pages, embedded content errors and the 500 internal server error, the survey found. Diane Smith, the group's research director, said she selected the sites because they are used in the Keynote Government Internet Performance Index from Keynote Systems Inc. of San Mateo, Calif. **The index includes sites of 10 Cabinet departments, the White House, both houses of Congress and several large agencies**. Smith said she visited each Web site for up to 15 minutes and explored as if she were unfamiliar with the agency. She stopped exploring at the first error, even if the 15 minutes were not yet up. **Twenty−five of the buggy sites had blank pages and internal server errors**. Smith said she found **three other sites with data errors, such as a wrong page link or bad data returned from a database query**.
Source: http://www.gcn.com/vol1_no1/daily−updates/22290−1.html

23. *May 29, Wired* — **Hacker exposes vulnerability in Cingular claims site.** Hacker Adrian Lamo found a security hole in a website run by lock\line LLC, which provides claim management services to Cingular customers. **Lamo discovered the problem last weekend through a random finding in a Sacramento, CA dumpster, where a Cingular store had discarded records about a customer's insurance claim for a lost phone**. By simply typing in a URL listed on the detritus, Lamo was taken to the customer's claim page on the lock\line website. Lamo was able to access individual claims pages containing customer's name, address and phone number, along with details on the insurance claim being made. **Altering the claim ID numbers in the URL gave Lamo access to some 2.5 million Cingular customer claims dating back to 1998**. Lamo said he had no intent of profiting from the exploit, just pointing out a security flaw. Cingular and lock\line closed the hole by Wednesday morning.
Source: http://www.wired.com/news/privacy/0,1848,59024,00.html

24. *May 29, eWEEK* — **Cyber−attack costs down, says survey. The percentage of organizations that detected unauthorized use of their systems fell to 56 percent from 60 percent a year earlier**, according to the latest "Computer Crime and Security Survey" from the Computer Security Institute and the FBI. The 2003 survey also shows that companies are still failing to report most of their intrusions and attacks to law enforcement. **Only 30 percent of the survey's respondents said they had contacted the authorities after an attack, a drop from 34 percent a year ago**. Negative publicity and fear that competitors would use the information to their advantage were the top two reasons organizations cited for failing to talk to

law enforcement after an attack. Among the most frequently seen attacks, viruses, laptop misuse and unauthorized access by insiders continued to lead the way, according to the survey. **The 530 organizations surveyed reported $201.8 million in losses this year; in 2002, 503 respondents lost $455.8 million**.
Source: http://www.eweek.com/article2/0,3959,1112190,00.asp

25. *May 29, IDG News Service* — **Microsoft revises two security bulletins.** Microsoft Corp. issued updates to security bulletins on Wednesday, fixing two recent software patches. **MS03−007, which was originally released in March, patched a serious vulnerability in a common Windows component, "ntdll.dll."** Microsoft's original patch fixed the problem for Windows 2000 Servers running Version 5.0 of the Internet Information Server (IIS), a platform that was actively being exploited when the patch was released. Microsoft acknowledged at the time that the vulnerability affected Windows NT 4.0 as well, but did not supply a patch for that platform, noting that WebDAV was not supported on NT 4.0. Observing that the WebDAV protocol was only one way to exploit the underlying vulnerability, **Microsoft updated the patch, adding fixes for the ntdll.dll vulnerability on the NT 4.0 platform and on the Windows XP platform, which is also vulnerable**. Microsoft also issued a fix for **MS03−013, a patch first released in April and then found to cause performance problems on the machines of some customers running the Windows XP operating system with the Service Pack 1 patch**.
Source: http://www.idg.net/go.cgi?id=805688

26. *May 29, National Journal's Technology Daily* — **Public−private partnership weighs homeland security technology ideas.** The Center for Commercialization of Advanced Technology (CCAT), a public−private research and development partnership funded by the Department of Defense, announced Thursday that it has received more than 100 responses to its recent solicitation for innovative technologies related to defense and homeland security. **Most applications submitted during the month−long solicitation, which closed May 15, were for emergency "first responder" technologies such as wireless communications devices, global positioning systems for tracking, and training software**. Other popular categories included explosive−detection technologies, chemical and biological detection systems, border−intrusion sensors, encryption decoding devices, and language−translation systems. **The center plans to announce the winners by mid−July**. Awards include product−development funding, marketing assessments, business planning and strategic consulting services.
Source: http://www.govexec.com/dailyfed/0503/052903td1.htm

Internet Alert Dashboard

Current Alert Levels

AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.F** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	80 (www), 137 (netbios−ns), 1434 (ms−sql−m), 20100 (−−−), 445 (microsoft−ds), 139 (netbios−ssn), 6346 (gnutella−svc), 0 (−−−), 17300 (Kuang2TheVirus), 41170 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *May 31, New York Times* — **Philippine camps are training al Qaeda's allies, officials say.** The southern Philippines has become the training center for Al Qaeda's Southeast Asia affiliate, Jemaah Islamiyah, drawing recruits from a number of countries, according to Western and Philippine officials. **For the last six to nine months, recruits mostly from Indonesia and Malaysia, but also a few from as far off as Pakistan and the Middle East, have received training at inaccessible, rough−hewn sites − basically a few huts and some tents − in a marshy region on the island of Mindanao, officials said.** The training is similar to what their older colleagues in terrorism got in Afghanistan when that served as Al Qaeda's base, they added.
Source: http://www.nytimes.com/2003/05/31/international/asia/31FILI. html

28. *May 31, Associated Press* — **Olympic Park bombing suspect in custody.** Eric Rudolph, the longtime fugitive charged in the 1996 Olympic Park bombing and in attacks at an abortion clinic and a gay nightclub, was arrested early Saturday in the mountains of North Carolina, a Justice Department official confirmed. **Sheriff's deputies in western North Carolina had spotted a man digging in a trash bin in the small town of Murphy at about 4:30 a.m., said Special Agent John Iannarelli in Washington. He said the man appeared to be homeless and when they deputies approached him, they recognized him as Rudolph.** Rudolph had been on the FBI's 10 Most Wanted list and had eluded a massive manhunt for five years, much of it in the western North Carolina mountains near where he was arrested Saturday. The FBI had offered a $1 million reward for his capture.
Source: http://www.nytimes.com/aponline/national/AP−Eric−Rudolph.htm l

29. *May 30, Associated Press* — **Riyadh bomb suspects sought in Pakistan.** Pakistani authorities are searching for two United Arab Emirates nationals suspected of involvement in the May 12 suicide attacks in Saudi Arabia, an official said Friday. **The two suspects are believed to have flown to the southern Pakistani city of Karachi earlier this month after the bombings in the Saudi capital, Riyadh.** An official at Pakistan's Federal Investigation Agency, which enforces immigration laws, said his department had received a letter from the Interior Ministry passing along a request by the United Arab Emirates to find and extradite the men.
Source: http://www.newsday.com/news/nationworld/world/wire/sns−ap−pa kistan−saudi−attacks,0,1575578.story?coll=sns−ap−world−headl ines

30.

May 29, Homeland Security &Defense — **Corporate security chiefs rank terrorism as a key worry.** Security directors at leading U.S. businesses rank the threat of terrorism among their top five concerns, but only one−third of them expect an increase in their budgets in the next three to five years, according to a new survey by Pinkerton Consulting & Investigations. Terrorism, which placed third in Pinkerton's 2002 survey, slipped to fourth place in this year's poll, after workplace violence, business interruption and Internet/Intranet security. Those categories also ranked in the top five in 2002.Company sectors included aerospace/defense, business services, consumer services, manufacturing, retail trade and utilities. **The poll also found that companies have dramatically cut the amount of money they planned to spend on security since 2002, citing tight or reduced budgets and a need to justify the effectiveness of security programs as the top reasons.**
Source: http://www.aviationnow.com/avnow/news/channel_hsd_story.jsp?id=news/corp05073.xml

31. *May 27, Office of the Auditor General of Canada* — **Canada Customs and Revenue Agency−managing the risks of non−compliance for customs. The Agency's most important accomplishments are collecting advance passenger information from most airlines to help target high−risk air travellers and improving the system for screening travellers at airports.** The Agency has also improved the targeting of in−transit marine containers by setting up joint targeting units with United States customs officials. As well, it has developed a plan to complete or update memoranda of understanding to better clarify roles and responsibilities with other entities on whose behalf it works at the border, and it has already signed five. **In other areas, more needs to be done. For example, customs officers screen people and commercial shipments at ports of entry on behalf of other entities, such as Citizenship and Immigration Canada and the Canadian Food Inspection Agency.** They need better information on the risk priorities of these other entities to help focus their efforts on areas of higher risk. Also, the Canada Customs and Revenue Agency is still not collecting the information it needs to determine whether its risk management strategy is working. Consequently it cannot assure Parliament that its actions have been effective. Report: http://www.oag−bvg.gc.ca/domino/reports.nsf/html/20030502ce. html
Source: http://www.oag−bvg.gc.ca/domino/media.nsf/html/20030502pr_e. html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.